知识管理论坛 ISSN 2095-5472 CN11-6036/C
Knowledge Management Forum
E-mail: kmf@mail.las.ac.cn
http://www.kmf.ac.cn

【学术探索】

“暗网”应用情况及监管方法研究

◎ 赵志云[1] 张旭[1] 罗铮[2] 袁卫平[3]

[1] 国家计算机网络应急技术处理协调中心 北京 100029
[2] 国家计算机网络应急技术处理协调中心广东分中心 广州 510665
[3] 国家计算机网络应急技术处理协调中心江苏分中心 南京 210003

摘要：[目的 / 意义] 通过对“暗网”在国内外的应用情况和发展趋势进行分析，对“暗网”可能带来的危害进行深入研究，以期为我国开展“暗网”监管提供参考。[方法 / 过程] 搜集国内外针对“暗网”研究的相关文献，通过对“暗网”的基本概念、特点和国内外应用情况进行调研总结，重点对“暗网”可能带来的危害、国内外针对“暗网”已有的监管措施和趋势进行分析。[结果 / 结论] 研究发现，美国、俄罗斯、英国等均投入力量开展针对“暗网”数据挖掘及监管的研究工作，但目前仍面临隐私保护被滥用和加密难破解等问题。提出加强“暗网”技术研究、推进加密服务立法和制定国际规则等监管建议。

关键词：暗网 恐怖袭击 数据安全 加密监管

分类号：G250.73

引用格式：赵志云 , 张旭 , 罗铮 , 等. “暗网”应用情况及监管方法研究 [J/OL]. 知识管理论坛 , 2016, 1(2): 124-129[引用日期]. http://www.kmf.ac.cn/paperView?id=22.

1 引言

巴黎系列恐怖袭击事件发生后，伊斯兰国恐怖分子联络策划所使用的“暗网”加密网络技术浮出水面，甚至有消息称“暗网”或将成为伊斯兰国恐怖分子的下一个避风港[1]。本文在介绍“暗网”基本概念、特点、应用情况的基础上，对“暗网”的危害和规管措施进行深入分析，并提出“暗网”的相关情况及监管建议。

2 “暗网”的基本概念及特点

2.1 “暗网”的基本概念

“暗网”又称深层网络（deep web），2001年伯格曼第一次使用该术语[2]。典型“暗网”主要分为以下几种类型，①建立在封包交换方式基础上的 I2P 等匿名网络，其上的应用程序可以安全匿名地相互通信，包括匿名上网、聊天、博客和文档传输。②建立在 P2P 分布式技术上的 Tor 等匿名网络，每一个用户的计算机变成加密的中继连接，当用户访问“暗网”时，没有任何一个中继或服务器能够获悉完整的连接痕迹。③建立在自组织机制上的 Firechat 等自组织匿名网络，各个节点通过特定自组织机制协同完成任务，能够适应各种网络条件，甚至是无网络条件[3-4]。与“暗网”对应的，是“明网”，也称表层网络。据“中关村在线”等网站分析，“明

作者简介：赵志云（ORCID：0000-0003-2089-1384），副高级研究员，硕士；张旭（ORCID：0000-0001-9361-8026），工程师，硕士，通讯作者，E-mail：zhangxu@cert.org.cn；罗铮（ORCID：0000-0002-7374-9050），研究实习员，硕士；袁卫平（ORCID：0000-0002-5925-6604），助理研究员，硕士。

收稿日期：2015-12-30 发表日期：2016-04-19 本文责任编辑：徐健

知识管理论坛，2016(2):124-129
DOI：10.13266/j.issn.2095-5472.2016.016

网”在数据量上只占到整个网络的约4%，“暗网”的数据量约有7.9ZB（1ZB=1亿TB），占整个网络的约96%[5]。

“暗网”之所以能成功，离不开美军的资金支持。1996年5月，美国海军研究实验室资助3位科学家在英国剑桥发表的名为《掩藏路由信息》的论文，提出“暗网”技术原型。2003年10月，该项目开源，称为Tor（洋葱路由），由非营利性组织电子前线基金会(Electronic Frontier Foundation,EFF）管理。但到2011年，其资金仍有60%来自美国政府。一般认为，Tor构建了“暗网”的基石和秩序。

2.2 “暗网”的主要特点

2.2.1 接入简单

只要掌握基本的“翻墙”技术，再下载一个几兆大小的软件，经过简单设置，就可以匿名接入“暗网”。此外“暗网”开发组织也在智能手机平台上发布了接入软件，更方便了“暗网”接入。

2.2.2 匿名性强

“暗网”通过采用分布式、多节点的数据访问方式和多层数据加密，为每一个数据包设计了一个加密的IP地址进行通信。要获取“暗网”的上网记录，必须破解“暗网”所使用的加密体制。

2.2.3 金钱往来隐蔽

在“暗网”上泛滥的非法交易，主要支付手段就是“比特币”。目前，在中国境内完全合法的比特币交易市场，1比特币可以轻松兑换数千元人民币，通过网上交易，从下单到提取现金，不超过30分钟。比特币交易的完全匿名性，保证了这些非法交易者的安全。

2.2.4 意识形态混乱[5]

“暗网”本身就是由有自由主义和无政府主义思想的人群建立的，用户中许多都是自由主义、无政府主义者。加上美军、美国政府的有意推动，“暗网”内自由主义倾向性非常明显。攻击社会主义国家制度，以及针对朝鲜和中国等国家领导人的攻击文章非常多。连贩毒、杀人都没人管的网络，其意识形态之混可想而知。

3 “暗网”的应用情况及危害分析

3.1 “暗网”应用情况

“暗网”中继节点在全球分布广泛且用户众多。2013年9月，据乔治城大学和美国海军研究实验室安全研究人员估计[6]，Tor在互联网的中继节点约有3 000个，大多数位于德国、美国和法国，同时中国、澳大利亚、荷兰、芬兰、奥地利、英国等国家也有分布；Tor日常的用户量约为95万，广泛分布于德国、中国、美国、意大利、土耳其、英国、日本等国家，其中德国、中国和美国的用户较多。

“暗网”被广泛应用在以下领域保护数据安全：①对通信安全要求较高的军事领域，可以有效防止敌人主动进行数据跟踪和数据分析，对于提供军事通信安全以及维护国家安全很有意义；②在电子商务中，起到保护商业机密和个人隐私的目的；③在云服务领域，使用“暗网”帮助用户建立加密通道，保护云服务使用者的隐私。

3.2 “暗网”带来的危害分析

不法分子利用“暗网”的匿名性进行非法交易甚至网络攻击：①利用“暗网”进行非法交易，其中包括毒品交易、儿童色情、武器交易、伪造身份、暗杀活动、出卖国家情报和不正当金融服务等。2013年10月被查封的著名贩毒网站“丝绸之路(Silk Road)”，就是利用“暗网”隐匿用户身份，逃避政府监管和执法[7]。安全研究人员在2013年1月还发现，不法分子通过“暗网”形成了价值数十亿美元的比特币网络交易黑市。“暗网”的存在，使得原本在公开互联网上就难以监管的网上勾联、秘密传输更加隐蔽，其匿名性强以及金钱往来隐蔽等特点，使得“暗网”具备成为最佳“买密卖密”平台的潜质。②利用“暗网”进行网络攻击。2012年12月，操控者通过Tor匿名网络对名为Skynet的僵尸网络进行控制，对多个政府网站发动DDos攻击。③不法分子通过“暗网”传输非法信息

和图片等，还采取利用匿名的 SMTP 产生垃圾邮件等方式进行蓄意破坏。另外，匿名"暗网"服务器也是网上其他一些非法活动的托管服务器。

"暗网"已成为潜在恐怖主义的"避风港"，伊斯兰国将"暗网"作为宣传机器以规避大规模政府审查。巴黎恐袭案发生后，有证据显示伊斯兰国恐怖分子的宣传机器 Al-Hayat Media Center 被快速转移到了"暗网"[8]。一个圣战论坛于 2015 年 11 月 15 日左右公布了一个镜像伊斯兰国恐怖分子各种数据的"暗网"地址，由于推特网和脸谱网迫于政府和公众压力大量封杀伊斯兰国恐怖分子的相关 ID，该论坛建议访问者使用具有"阅后即焚"特点的自由开放源代码软件 Telegram。此类软件不仅加密算法复杂，有将消息自动销毁的功能，而且不会把内容储存在服务器里，堪称"恐怖隐身"完美渠道。巴黎恐怖袭击事件发生以后，Telegram 上被查出至少有 78 个伊斯兰国的群组 [8] 。在新型反恐战争下，这样的公司服务已经对国家安全构成了威胁。由于 Telegram 拒绝与安全部门合作，目前已被部分国家政府封闭。伊斯兰国恐怖分子"明暗游击"的网络策略，让世界各地安全部门头疼不已。美国中央情报局局长布伦南指出，如今的恐怖活动已不易被政府当局识破，恐怖分子已经学会了相关新技术，他们的安全网络通信能力显著提升。

境内"百度贴吧"等论坛有关"暗网"入口等技术问题成为高频词汇。与前几年我国境内尚未发现大规模网民在"暗网"中出现的情况相比，"暗网"的概念近来受到诸多网民关注，随着网民突破我国互联网管控手段的提升，越来越多的网民也参与到"暗网"的使用中。通过"百度贴吧"搜索"暗网"可直接看到有网民创立"暗网吧"介绍"暗网"入口、接入方法等技术贴，还有网民创办 Tor 使用交流 QQ 群，甚至有网民直接发布"暗网"相关图片和内容以吸引眼球，介绍"黑死病"等"暗网"网站的服务内容，包括武器、毒品、暗杀等。还有网民声称"暗网"可以进行器官买卖、人口贩卖等服务。

加密通信网络被使用于香港"占中"等群体性事件。在香港"占中"活动中，FireChat 短短不到一天就被下载 10 万次，并成为"占中"组织开展活动的主要通信和传播工具。其具有无中心节点、网状连接的特点，在密集区域可以快速自行组网实现大面积的信息传播 [9] 。台湾地区的"太阳花学运"中也使用 FireChat。甚至有网民称 FireChat 已成为公民运动必备的软件。在今年香港政改表决期间，多名泛民议员开始使用具有"阅后即焚"功能的加密通信软件 Telegram 沟通。

4 针对"暗网"的规管措施及问题

4.1 针对"暗网"的规管措施

巴黎恐怖袭击发生后，相关私密信息传输监管问题引发各国关注，法国、英国、美国等国均加强了相关立法和投入。法国国会为应对私密信息传输正式授权法国政府可以在紧急状态下关闭任何涉及恐怖主义行径的互联网公共通信服务 [10] 。美国联邦通信委员会 FCC 建议美国重新修订窃听法案，扩大窃听范围，还有官员呼吁科技公司放开包括通话、短信和电子邮件等加密通信的访问权限，FBI 和 CIA 也开始进一步要求苹果和谷歌开放智能机通信加密的后门 [11]。英国则将向军情五处、军情六处和政府通信总部增拨 15% 的经费，计划在 5 年内投入 19 亿英镑用于打击网络袭击和网络恐怖活动，并集中全英国顶尖专家成立一个新的国家网络中心 [12]。德国政府则预计在情报领域增加 500 个工作岗位 [13] 。韩国、越南等国也纷纷加强和推动涉及网络恐怖袭击、通信秘密保护等立法工作 [14-15] 。

各国投入高额成本打击"暗网"，但前景并不乐观。英国政府通信总部对高校的资助在不断增加。其中 Heilbronn 研究所是一家由多所英国大学的科研精英合作的机构，其主要精力即为间谍部门指导的追踪研究项目。2014 年 2 月，俄罗斯总统普京通过了一项法案，允许政府在必要时期切断俄罗斯国内的整个互联网，而

知识管理论坛，2016(2):124-129
DOI：10.13266/j.issn.2095-5472.2016.016

且强制要求日均访问量超过 3 000 人次的网站所有者向政府备案，放弃匿名权。美国联邦调查局、美国缉毒局、美国烟酒枪炮及爆裂物管理局和国家安全局等美国政府部门为攻入"暗网"中的非法网站，花费每年都在数千万美元之巨。而美国国防部先进研究项目局则在 2015 年初发布"暗网"搜索引擎 Memex，通过深度挖掘"暗网"，获取 Google 搜索和其他商业搜索引擎未能涉及到的所有隐秘信息，但该搜索引擎只面向美国军方。斯诺登泄露的一份美国国家安全局文件(2012 年 6 月的文档)显露出，美国国家安全局对破解"暗网"的前景并不感到乐观，甚至明确表示："将永远不可能完全揭开所有'暗网'用户的真实身份"[16]。而被抓获的"丝绸之路"创办者，也并非是在"暗网"上露出了"马脚"，而是因为在普通因特网上留下了太多关于"丝绸之路"网站的招聘和代码求助信息。

4.2 当前监管方面的主要问题

各国都积极开发针对"暗网"的搜索平台，但仍存在法律争议和技术瓶颈。2014 年，用于黑市搜索的网站 Grams 上线。2015 年，美国黑客维吉尔•格里菲斯宣布对公众开放的"暗网"搜索 Onion.City[17] 问世，通过它能轻易地访问隐匿在"暗网"中的大量信息。但这些搜索引擎是否违法，暂时存在争议。

4.2.1 云服务将使政府追踪"暗网"上的不法行为变得更加困难

据 BBC 中文网的相关报道，专家表示使用云服务将使政府追踪"暗网"上的不法行为变得更加困难。比如，来自亚马逊名为 EC2，即"弹性计算云"能够支持虚拟计算机的功能，而"洋葱暗网"的开发者号召人们加入这一服务，以便运行网桥，即用于两个或多个网络之间的互连设备或是秘密网络的虚拟点，通讯可以沿此路径进行。有了云服务的支持，将很容易创建出相当数量的网桥。这将催生出更多、更好的"藏匿地点"，匿名网络的数量也将越来越多。

4.2.2 隐私保护成为"暗网"被滥用的理由

"暗网"是互联网技术蓬勃发展的产物，也代表了部分网民匿名上网、保护隐私的正当需求，但也充斥着非法犯罪交易和意识形态攻击。如何处理隐私保护与打击"暗网"犯罪行为成为矛盾而难解的问题，美国官员曾不留情面地质询欧洲各国因为过度关注隐私议题，而牺牲公共安全保卫能力。2015 年 2 月美国成立新的网络反恐机构——网络威胁情报整合中心时，奥巴马总统许诺将推进更为严格的网络安全立法。法国议会在 2015 年通过了反恐新法，包括对网络平台进行更加严格的监控，对涉嫌恐怖主义信息宣传予以惩罚。但是目前在各国均没有对访问"暗网"的行为在法律中进行详细的约束。

4.2.3 "暗网"接口的隐蔽性较强，移动终端的监测更为困难

"暗网"通信建立在互联网之上，监控"暗网"接入软件下载情况，能够有效摸清使用"暗网"的行动动向。但是，目前"暗网""接口"信息的发布较为隐蔽，通常采取私聊或一对一方式传播，而对通过 BT 下载和网盘分享等方式规避监管暗中提供"暗网"接入软件的，要摸清下载人的身份和目的也存在较大难度。特别是移动终端的数量大幅增长以后，智能手机平台"暗网"接入软件的下载和使用也会更为频繁，这也提高了追踪下载人的行为动向的成本。

5 加强针对"暗网"的监管建议

由于"暗网"能够提供有害信息穿透、真实网络身份隐藏、电子黑市交易等存在较大安全隐患的服务，为了更好地对抗有害"暗网"，建议下一步开展工作如下：

5.1 加强"暗网"技术研究，将其"为我所用"

"暗网"是互联网技术蓬勃发展的产物，也代表了部分网民匿名上网、保护隐私的正当需求，但因为其充斥着非法犯罪交易和意识形态攻击，更可能成为敌方策反我军相关人员的"暗道"。应当给予足够重视，技术上加以研究，加强保密管理，打好防范"暗网"泄密的主动仗。另外，"暗网"在技术结构上能有效防范网络刺探攻击和网络流量分析攻击，研究"暗网"构

建技术对我军建设保密指挥、办公网络，也具有较强的借鉴意义。

5.2 对国内互联网加密服务推进立法

为有效解决“暗网”中加密应用带来的互联网监管挑战，建议国家有关部门加强互联网加密服务监管的相关立法工作。首先，对互联网信息内容安全监管工作进行明确定位并制订相应的法律依据，明确监管部门、服务提供商、网络提供商、用户四方的权利和义务，落实网络信息安全责任。在此基础上，进一步明确和细化互联网加密服务监管相关法律法规，借鉴国际上反恐、技侦、打击违法犯罪、儿童保护、知识产权保护等方面的共同需求和做法，如明确要求提供加密服务的企业必须在对数据进行加密和压缩之前提供监管接口，以满足政府管理部门的需求。

5.3 制定国际规则约束滥用技术优势进行的监控等行为[18]

美国国家安全局在 2013 年 8 月份承认对 Tor 网络进行监听，并已经将其所截获的信息与其他机构共享，其中包括美国缉毒局和联邦调查局，并声称其主要用于破获关于毒品和儿童色情的案件。但是对于这种网络监控行为是否侵犯他国主权、是否侵犯了各国民众的基本权利以及是否符合国际法等，却避而不谈。为了从根本上保障 Tor 在互联网上的积极应用，避免美国等技术大国对网络的私用和滥用，有必要推动建立多方、透明和民主的互联网治理机制，并加快制定网络空间行为规则，规范各类主体行为，加快建立网络空间新秩序。

参考文献：

[1] 暗网将成为伊斯兰国的下一个避风港 [EB/OL]. [2015-12-20]. http://www.freebuf.com/articles/86048.html.
[2] RAGHAVAN S, GARCIA-MOLINA H. Crawling the hidden Web[EB/OL]. [2015-08-12]. http://ilpubs.stanford.edu:8090/456/1/2000-36.pdf.
[3] 孙玲 , 潘京 . “暗网”: 互联网世界的灰色地带 [J]. 国外科技动态 , 2005(12): 36-39.
[4] 刘鑫 . 基于 Tor 网络的匿名通信研究 [D]. 上海 : 华东师范大学 , 2011.
[5] 罪恶的天堂? 带你了解搜索不到的暗网 [EB/OL]. [2015-12-20]. http://oa.zol.com.cn/494/4945765_all.html.
[6] JOHNSON A, WACEK C, JANSEN R, et al. Users get routed traffic correlation on tor by realistic adversaries[C]// Proceedings of the 2013 ACM SIGSAC conference on computer & communications security. New York: ACM, 2013:337-348.
[7] “丝绸之路”涉嫌贩毒 [EB/OL]. [2015-01-14].http://www.techweb.com.cn/internet/2015-01-14/2115554.shtml.
[8] After Paris, ISIS moves propaganda machine to Darknet[EB/OL].[2015-12-20].http://www.csoonline.com/article/3004648/security-awareness/after-paris-isis-moves-propaganda-machine-to-darknet.html#tk.rss_all.
[9] 香港“占中”事件中的新媒体使用 [EB/OL]. [2015-12-20]. http://www.neweyeshot.cn/archives/15961.
[10] 法国国会授权政府可随时关闭网络 [EB/OL]. [2015-12-20]. http://world.huanqiu.com/exclusive/2015-11/8014730.html.
[11] FCC 主席 : 巴黎袭击后 FBI 要更多窃听权力 [EB/OL]. [2015-12-20]. http://www.cnbeta.com/articles/449539.htm.
[12] 英国向三大情报机构额外拨款应对恐怖袭击威胁 [EB/OL]. [2015-12-20]. http://www.chinanews.com/gj/2015/11-16/7626267.shtml.
[13] 情报部门“招兵买马”对抗恐怖主义与极右翼 [EB/OL]. [2015-12-20].http://www.dw.com/zh/%E6%83%85%E6%8A%A5%E9%83%A8%E9%97%A8%E6%8B%9B%E5%85%B5%E4%B9%B0%E9%A9%AC-%E5%AF%B9%E6%8A%97%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E4%B8%8E%E6%9E%81%E5%8F%B3%E7%BF%BC/a-18851449.
[14] 韩媒 : 全球反恐时代韩国政府不能继续“隔岸观火”[EB/OL]. [2015-12-20]. http://finance.chinanews.com/gj/2015/11-17/7626853.shtml
[15] 越南要求严惩利用社交网络煽动恐怖主义的用户 [EB/OL]. [2015-12-20]. http://www.apdnews.com/XinHuaNews/264368.html.
[16] 隐匿的“暗网”帝国 [EB/OL]. [2013-11-18]. http://www.nbweekly.com/news/world/201311/35013.aspx.
[17] Onion link[EB/OL]. [2015-12-20]. http://onion.link/.
[18] 张伟丽 . 洋葱路由应用面临的挑战与对策建议 [J]. 电视技术 , 2015, 39(1): 103-105.

作者贡献说明：
赵志云： 拟订论文主题，修改论文终稿；
张旭： 研究暗网监管细节，负责起草论文；
罗铮： 分析暗网概念、特点，梳理暗网监管措施；
袁卫平： 研究暗网应用情况。

ChinaXiv合作期刊
知识管理论坛，2016(2):124–129
DOI：10.13266/j.issn.2095–5472.2016.016

The Study of Utilization and Regulations of the Deep Web

Zhao Zhiyun[1] Zhang Xu[1] Luo Zheng[2] Yuan Weiping[3]
1 National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029
2 National Computer Network Emergency Response Technical Team/Coordination Center of Guangdong, Guangzhou 510665
3 National Computer Network Emergency Response Technical Team/Coordination Center of Jiangsu, Nanjing 210003

Abstract: [Purpose/significance] The "deep web" encrypts information for privacy protection, but it was used by IS terrorists to launch attacks in Paris. Except for analyzing the utilization and regulations of the "deep web", this paper also analyzes its detriment and proposes regulation methods of the "deep web". **[Method/process]** This paper investigated the concepts characteristics and utilizations of Deep Web, especially analyzes its detriment and regulation methods and trends. **[Result/conclusion]** Many countries including the USA, Russia and England conduct researches on data mining and regulations of the "deep web". The problems in this domain include the abuse of privacy and challenges in decryption. This paper proposes to regulate the "deep web" in three aspects by strengthening researches on the "deep web", pushing legislation and making international rules.

Keywords: deep web terrorist attack data safety encryption regulation